Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

DOS Attack Detection Using Fisher Score Based Feature Selection and Gated Recurrent Network in Computer Network

[1]Sanjeev Kumar, [1]Rajiv Singh, [2]Dr Ankit Agarwal
[1]Banasthali Vidyapith, [1]Banasthali Vidyapith, [2]Dr Akhilesh Das Gupta Institute of Professional Studies
Rajasthan, India Rajasthan, India Delhi, India
sanjunic@hotmail.com , jkrajivsingh@gmail.com cs.ankit11@gmail.com

ARTICLE INFO

Received: 24 Dec 2024
Revised: 12 Feb 2025
Accepted: 26 Feb 2025

ABSTRACT

Security threats is determine to be a significant issue caused in computer network due to malicious behaviour. Prevailing of these abnormal activities is due to injection of various cyber-attack by the attackers. A solution for this problem is to introduce Artificial Intelligence (AI) system for achieving effective DOS attack detection. Machine learning algorithm was used initially to detect DOS attacks. But low detection rare is a major drawback faced on using this algorithm. To overcome this issue, deep learning based DOS attack detection model is developed using Gated Recurrent Network (GRU). In this proposed model, initially the information regarding data storing and accessing by the users is obtained. The acquired data is pre-processed using mini-max normalization. Then, from the pre-processed data the features necessary for detection using selected using filter based technique namely fisher score. These selected features are given as input into GRU to detect DOS attack and non-attack data. The non-attack data is further encoded using Modified Random Linear Network Coding (MRLNC) and finally the encoded data using MRLNC is stored in cloud. Whereas in case of DOS attack data an alert message is provided to the user regarding the attack. Proposed deep learning based DOS detection model is implemented to evaluate its performance. Some of the statistical metrics such as accuracy, error, precision and sensitivity attained for proposed DOS attack detection model is 93%, 7%, 94% and 92%. This evaluation shows that improved DOS attack detection is achieved using proposed GRU model.

Keywords: DOS attack, network traffic, gated recurrent network, deep learning, modified random linear network coding, cyber-attack detection.

1. INTRODUCTION

In modern era, the use of internet is drastically increasing due to lot of advancement attained in the domain of communication technology. Many devices that are utilized for individual purpose as well as for industrial application utilize internet as a source for communication [1]. By means of utilizing internet enabled devices the living standard is increasing all over the globe. However, information threat is still a major concern faced in this devices functioning with internet which is needed to be solved. The information threats are mainly due to cyber-attacks which is generated from different sources [2]. Among various cyber-attacks, Distributed Denial of Service (DDOS) attacks and Denial of Service (DoS) is most frequent and common attack faced in various network resources. Generally, the DOS attacks are done in two stages in which the first stage is intrusion and second stage is attack [3]. At intrusion stage, the instalment of DOS attack tools upon various network host is performed. While at attack stage, the attacking is triggered upon the focused network host [4].

With the help of these host, the attackers generate massive traffic for forcing the target routers. By means of this traffic the resources as well as bandwidth of the victim machine are disbursed [5, 6]. Therefore, the service requested by legitimate users is not provided by the target resources which ultimately result in deny in service. To solve this cyber-attack prevailing within the network Intrusion Detection System (IDS) and firewall. Using these designed systems, the presence of traffic and abnormal activity in the network can be identified [7]. The abnormal activity within the network can be categorized into two ways. One is anomaly detection and another one is misuse detection

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[8]. Based on the attack detection technique these two methods are categorized. In case of misuse detection, the determination of attack model is achieved when a signature related to malicious transaction matches [9]. Whereas in case of anomaly detection, the corresponding of data towards estimated behavior of network is not achieved.

In spite of advancement made in cybersecurity system still complex techniques are used by attackers which are quite challenging to be solved by existing IDS and firewall. So, the researchers are aiming to utilize Artificial Intelligence (AI) system to detect the presence of DOS in network flow [10]. Machine Learning (ML) algorithm are most commonly utilized AI technique for prediction. Some of the ML technique used for DOS detection are Support Vector Machines (SVM), Naive Bayes (NB), Decision Trees (DT) and K-Nearest Neighbour (K-NN). These approaches' usage in intrusion detection systems is reliant on understanding how to reflect their beneficial characteristics in network data [11, 12]. As a result, the ML uses the features that were extracted from the raw data by concentrating on the structure assets and data presentations. A substantial incidence of false positives is produced when ML algorithms are used to detect network anomalies.

To address this issue, deep learning techniques are employed to automatically extract complicated features. The ML algorithms favour network traffic to cope with anomaly detection more successfully. The deep learning models employ supervised and unsupervised techniques to automatically extract hierarchical and layer-based information. To enhance the quality of the data and the classification outcomes of ML algorithms, feature size reduction techniques are employed to reduce the number of features. A subset of related attributes must first be extracted from the network traffic dataset in order to detect effective DDOS network anomalous activity. Second, the top methods should be chosen in order to enhance classification outcomes and speed up classification.

The major contribution of this research work is listed below,

- Deep learning based approach is designed to detect the presence of DOS attack within the network which is caused due to creation of traffic by cyber attackers. IDS and firewall are commonly used techniques but it faced difficulty in solving complex cyber-attacks.
- Collected data from users is of raw data and it result in inaccurate detection. So, these raw data are pre-processed using min-max normalization technique to normalize the data within certain range.
- Redundant features needed for classification is selected using fisher score which is a filter based feature selection techniques.
- Selected features are fetched into GRU which a deep is learning approach used to categorize attack and non-attack data. Non-attack data is further encoded using MRLNC and then stored in cloud. Attack data is categorized into different type of attack and an alert message is sent to the user.
- Improved detection accuracy with less false positive rate is determine to be achieved using this proposed deep learning based DOS detection model.

The remaining portion of the paper is organized as follows, section 2 contains the articles reviewed based on DOS attack detection using deep learning approach. Section 3 comprises the proposed DOS attack detection model using GRU. Section 4 comprises the results obtained through implementing the proposed model. Finally, section 6 concludes the paper.

2. LITERATURE REVIEW

DOS attack detection is considered as mandatory to overcome various security threats causedin the network flow by cyber-attacks. To detect DOS attack within the network various machine learning algorithm is utilized. But due to the introduction of complex attacking procedure by attacker. DOS detection using machine learning algorithm is difficult. So, deep learning based DOS attack detection is developed. Some of the deep learning based DOS attack detection techniques is reviewed below.

Amit V. Kachavimath et al., [13] developed deep learning technique for detecting DOS attack within cloud system. Detection of DOS attack in case of real time was determine to be challenging. To address this problem, initially the presence of traffic within the network must be analysed and then using the acquired traffic attributes the difference in activity was detected. Alternatively, the activity difference within the network can be detected using various machine learning algorithm to find DOS attack. However, these algorithm attained time delay as well as less detection

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

rate. To solve this issue high level feature from the acquired traffic in the network was analysed using deep learning approach to detect DOS attack with high detection rate.

Mohamed Amine Ferrag et al., [14] developed an effective intrusion detection system using deep learning technique to solve DOS attacking issue within agricultural sector. As many numbers of IoT devices were deployment in open area as in case of agriculture they were frequently prone to various security threats. So, the researchers working on security threats were focusing to protect these devices from various cyber-attack like DOS attack caused by adversary. Through injecting DOS attack into the system, the service of the device become unavailable and lot of false data were included which created unsafe agricultural equipment. These false data injected into the system showed that the equipment was safe but in case of reality the equipment seemed to be unsafe. To solve these issues in agricultural sector, deep learning based DOS attack detection model was introduced. Here, three deep learning models like RNN, DNN and CNN was utilized.

Congyuan Xu et al., [15] developed modified deep neural network for predicting low rate DOS attack. In case of low rate DOS, the request provided at low rate was utilized to perform the function relevant to the network resources and also provide robust concealment. Some of the existing detection model developed based on signal analysis was found to be quite challenging for detecting low rate DOS attack due to presence of oscillating legitimate traffic. So, in this developed system modified DNN was designed through couplinhg DNN with GRU for detecting low rate DOS. The developed hybrid model was simulated using real traffic data iun which the extraction of features was not done manually but effective low rate DOS detection was achieved even in oscillating HTTP traffic. The average detection rate for the developed model was found to be 98.68%.

S. Ramesh et al., [16] also developed modified DNN using optimization algorithm for analysis DOS attack in Wireless Video Sensor Network. Generally, multiple attackers created attack within the network which was referred to as distributed attack. This kind of distributed attack causes heavy damage to the network functionality when compared to attack caused a single node. To recover the network from DOS attack threats, an improved machine learning algorithm was utilized. However, low detection rate was major drawback faced on using machine learning algorithm. So, to overcome this issue modified DNN using adaptive particle swarm optimization was developed. Efficacy of the developed system was analysed through measuring throughput, network length, latency, energy consumption and packet transmission.

M. Premkumar et al., [17] designed deep learning enabled defense mechanism for predicting DOS attack in WSN. Due to lack of synchronization among nodes while data transmission in WSN they were heavily prone to DOS attack. To detect DOS attack within WSN system deep learning enabled defence mechanism was developed. Using this mechanism, the detection and isolation of attack was done in data forwarding phase. Some of the algorithm included for efficient detection of DOS attack was flooding, homing, jamming and exhaustion. Simulation analysis performed on the developed system showed accurate isolation of various attacks specifically DOS attack. Along with that it also achieved improved packet delivery ratio, throughput and detection rate.

Bhuvaneswari AmmaN.G et al., [18] developed Deep Radial Intelligence (DeeRaI) coupled with Cumulative Incarnation (CuI) technique for detecting DOS attack in online services. The intelligence derived from the radial basis function was learned using various degrees of abstraction in this created DeeRaI technique. The DeeRaI network, in which the acquired knowledge was passed on to the following generation, has its weights optimised by the suggested CuI. The suggested approach was contrasted with current classifiers and cutting-edge attack detection systems in experiments on benchmark datasets. The performance evaluation demonstrated that the suggested approach outperforms other current approaches in terms of results. In addition, it was clear that the suggested method converges quicker and yielded the optimal weights when compared to the current optimization techniques.

Some of the deep learning based DOS attack [24, 25] detection techniques was reviewed in this section. Based on these articles it was found that emergence of various DOS attack within IoT, WSN and another network system can be analysed. These DOS attack was created due to presence of traffic within the network. Using these existing deep learning approaches low detection rate was achieved due to complex attacking strategy performed by the attackers. So, to achieve accurate prediction wit high detection rate efficient deep learning algorithm must be developed.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. PROPOSED METHODOLOGY

Internet usage is increasing dramatically all over the globe and various devices which are utilized for individual as well as industrial applications communicates with the assist of internet connection. However, these devices enhance the living standard of people the information communicated using these devices via internet are frequently throttled to various cyber-attack. Among them DoS attack is most prominent attack which is experienced in many devices linked with internet. Intrusion Detection system is used to find abnormal activity within the network that contributes to cyber-attack. Lot of advancement were made in cyber security technology still complex attacking strategy used by the intruders are very tricky to be solved using IDS. To face complex attack in network system researchers are focusing on using various machine learning algorithms. However, these machine learning does not achieve accurate detection in case of huge and complex data. Thus, deep learning based DoS detection model is proposed in this research. Figure 1 illustrates the proposed DoS detection model using deep learning technique.

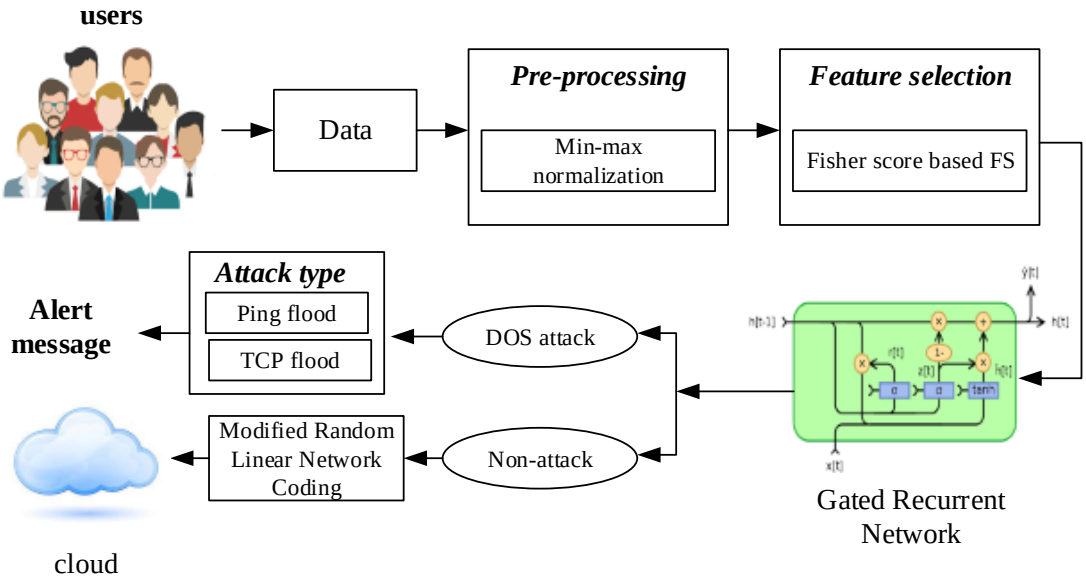

Figure 1: proposed DOS Attack Detection Model using Deep Learning

At the beginning of the process the information regarding the data transmission between multiple users through internet is collected and further structured as a dataset. The acquired dataset consists of raw data which causes difficulty during detection using the classifier. So, prior fetching these data into the classifier these acquired raw data is pre-processed using various techniques. Min-max normalization is a pre-processing technique which is used to normalize the data within certain range. The normalized data is sent for feature selection process in which the essential features are selected using fisher score based feature selection technique. Processed data is fetched as an input into Gated Recurrent Unit (GRU) for classifying between presence and absence of DoS attack. The non-attack data is then sent as an input into Modified Random Linear Network coding (MRLNC) for compressing and encoding the data and the finally obtained non-attack data is stored in cloud. On the other hand, the data which consist of attack is further categorized into different types of DoS attacks and an alert message is sent to the user. Based on this proposed deep learning model the DoS attack detection can be done effectively. Sequences of steps involved in this proposed DoS detection model is explained below.

3.1 Pre-processing

The data is not in a specific range so pre-processing technique is used to fit the dataset in an exact range. Several approaches are available for normalization of dataset [19]. Among them Min-Max normalization is more efficient.

Min-Max Normalization

Normalization approach convert a value from σ toσ^* that is suitable in the range of [A, B] [20]. Its mathematical expression is given below.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

$$\sigma^* = \frac{\sigma - \sigma_{min}}{\sigma_{max} - \sigma_{min}} \quad (1)$$

The data is normalize to give an equal weight of all attributes. After the normalizing process the process of feature selection is performed using filter based method which is explained below.

3.2 Feature selection

Normalized data is next sent for feature selection process in which the optimal features necessary for classification is selected. Two feature selection techniques such as filter and wrapper based technique are widely utilized. Various filter based feature selection technique such as chi square, correlation dimension and so on. However, these technique does not function effectively in case of high dimension data. To solve this issue, in this current work fisher score based feature selection technique is utilized.

Fisher-score based technique

Fisher score is a feature selection technique which helps in selecting optimal features from the dataset. This fisher score technique performs better in case of data with high dimensionality which another existing algorithm fails. Using fisher score the set of features is obtained in which the distance related to data point containing dissimilar class must be far and on the other hand the distance related to data point containing similar class must be closer [21, 26]. Consider a data matrix $X \epsilon R^{m \times n}$ containing m features is given as input. This taken data matrix is further reduced to $Z \epsilon R^{f \times n}$ in which f represent the selected features. Expression used for calculating the fisher score is given below.

$$F(Z) = tr\{(\widetilde{sb})(\widetilde{st} + \gamma I)^{-1}\} \quad (2)$$

In eqn (2) γ denotes the regularization parameter which is said to be positive, $\widetilde{sb}$ represents the scatter matrix between classes and total scatter matrix is represented as $\widetilde{st}$. Formula used to calculate $\widetilde{sb}$ and $\widetilde{st}$ is given in eqn (3) and (4)

$$\widetilde{sb} = \sum_{k=1}^{c} n_k (\tilde{\mu}_k - \tilde{\mu})(\tilde{\mu}_k - \tilde{\mu})^T \quad (3)$$

$$\widetilde{st} = \sum_{k=1}^{c} n_k (z_i - \tilde{\mu})(z_i - \tilde{\mu})^T \quad (4)$$

In eqn (3) and (4) μ represents the entire mean vector related to feature, $\tilde{\mu}_k$ represents the mean vector of k^{th} class and following that n_k represents the size of k^{th} class, z_i represents the selected set of features. So, the mathematical expression used to calculate fisher score is given in eqn (5).

$$FS(X^j) = \frac{\sum_{k=1}^{c} n_k \left(\mu_k^j - \mu^j\right)^2}{\left(\sigma^j\right)^2} \quad (5)$$

In eqn (5) μ_k^j represent the mean of j^{th} feature in k^{th} class, μ^j represents the mean of entire j^{th} feature and σ^j represents the standard deviation of entire j^{th} feature. Based on this fisher score optimal features necessary for classification are selected from the dataset.

3.3 DoS attack detection using deep learning

Features selected using fisher score is then sent for detection of DOS attack using deep learning algorithm. In most of the traditional DOS attack detection system machine learning algorithm were utilized. But, using these ML algorithm accurate detection is not attained so, the researchers are moved on using deep learning algorithm which is the advance of ML. Among various deep learning algorithm GRU is used in this current work for DOS attack detection.

Gated Recurrent Unit (GRU)

GRU is designed through making some improvement in the structure of RNN and this GRU model is mainly used for predicting time series data. In case of traditional network model initially the input layer is connected with the hidden layer and then ultimately to the output layer. In case of every network model the direct node present in each layer is linked whereas other nodes remain disconnected. Main advantage in using RNN is that it has the ability to remember prior information and further utilize it in the estimation of current output. The nodes present in between the hidden

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

layers was found to be disconnected. On the other hand, the input related to the hidden layer encloses output for the last moment along with the output of the present input [22, 27]. This scenario of hiding the output of last moment can solve the issue of direct connection of node in each layer.

In spite of its advantages it possesses certain limitation during increase in number of hidden layers. As number of hidden layers increases the previous information stored in the node may get diminished or disappeared during back propagation so, they are not suitable for data samples consisting of long sequence. To solve this issue LSTM is developed which is the improvement version of RNN used in case of long term series. The general structure of LSTM consists of three gates such as forget gate, input gate and output gate which are connected to the neuron. The function of forget gate is to manage the acceptance regarding previous information and it is also termed as degree of forgotten. Following that the function of input gate is to manage the new input information and at last the function of output gate is to manage the filtering of current unit state.

Even though LSTM solves the issue of handling long sequence still its structure is complex and difficult to understand. Figure 2 illustrates the general architecture of GRU.

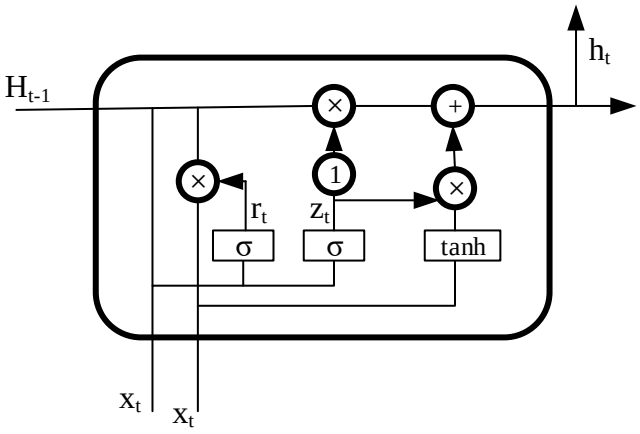

Figure 2: General Architecture of GRU

GRU an improvement of LSTM is developed which consist of simple structure but maintains the effectiveness of LSTM. Structural model of GRU consist of two gates namely the reset gate and update gate. The main intension for utilizing update gate is to manage the bringing of historical state of information to the present state. Presence of greater value for update gate shows that more state of information is obtained from prior moment. Following that the role of reset gate is to manage the deletion of status information obtained from prior moment. Presence of lesser value for reset gate shows that many numbers of status information is deleted. Unit state is combined with the output state at same time and made into one state.

Combining unit state and output state into one state is denoted as h. x_t denotes the present input of the model and the state which is offered by the node present in the prior hidden layer is denoted as h_{t-1}. Along with the state its corresponding information regarding the prior node is also provided. So, the output from the node in the hidden layer can be calculated using these two variables such as h_{t-1} and x_t along with managing the two gates. Additionally, the information sent to the succeeding node in the hidden layer can also be found. Mathematical expression used to represent two gates such as update gate and reset gate along with its state is given in eqn (3) and (4)

$$u_t = f(w_u(x_t, h_{t-1}) + b_u) \quad (3)$$

$$r_t = f(w_r(x_t, h_{t-1}) + b_r) \quad (4)$$

Here, u_t and r_t denotes the gate control such as update gate and reset gate, f represents the sigmoid activation function, w_u and w_r are the connection weight of neurons. The range of value for f can be given between zero and one. Using this range of value the gating signal can be obtained through gating. Once the gating signal is obtained

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

initially the rest gate is used to obtain the reset data and further merged with the activation function namely *tanh* to obtain $\widetilde{h_t}$ and its corresponding mathematical expression is given in eqn (5)

$$\widetilde{h_t} = f(w[r_t \times h_{t-1}, x_t]) \quad (5)$$

Here, f represents the *tanh* function which is found to be in the range in between -1 and 1. In this case the input data is provided and followed by that the information in the hidden node is managed. Whereas in case of update phase the function of remembering and forgetting is done and it is controlled with the help of update gate. Mathematical expression used to represent *tanh* function for update gate is given in eqn (6)

$$h_t = (1 - u_t) \times h_{t-1} + u_t \times \widetilde{h_t} \quad (6)$$

Where, z_t is found to be in the range between zero and one. If value of z_t is closer 0 then it shows that lots of data is forgotten and if value of z_t is closer to 1 then it represents that more data is reserved in the memory. So, using update gate both the function of memorizing and forgetting can be performed simultaneously. Thus, the function used for denoting the degree of forgetting for the hidden state is similar to that of forget gate and some amount if irrelevant information are forgotten. This function $(1 - u_t) \times h_{t-1}$ represents the degree related to selective memory of information in present node and it is quite similar in selecting some relevant information. Using this GRU model the prediction of attack and non-attack data in the devices communicating through internet can be performed effectively. As using GRU based deep learning approach the data are classified into presence and absence of DOS attack.

3.4 Non-attack DOS class

Data which are predicted as attack free class is further processed using MRLNC technique to compress and encode the data prior storing in cloud storage system. The process involved in network coding technique for compression and encoding the data is explained below.

Process of encoding is done on non-attack data prior to storing in cloud because there is also possibility for security concern in cloud storage also and so to secure data from attackers within cloud storage this encoding technique is utilized. Encoding technique used in this current work was MRLNC. Modified RLNC is nothing but including data compression prior to encoding process as data transmitted in large volume can cause increased transmission delay. Detailed description regarding MRLNC is given below.

Modified Random Linear Network Coding (MRLNC)

At first, process of data compression is achieved in MRLNC before transmitting the data to cloud. Consider the data acquired from the user within some time period is denoted as $(X = x_1, x_2 \ldots \ldots x_n)$. For data compression a technique namely uniform random Bernoulli matrix is utilized and this Bernoulli matrix is represented as B. Within this Bernoulli matrix the elements present can be given using equation (7)

$$b_{ij} = \begin{cases} -\frac{1}{\sqrt{n}}, & n < 0.5 \\ \frac{1}{\sqrt{n}}, & n \geq 0.5 \end{cases} \quad (7)$$

Here, $b_{ij} \in B$ in which b_{ij} represents the element within the matrix. After finding the matrix B the row of the matrix is taken to be compression matrix as it does not change or cause any loss for the initial information content. Data compressed using m dimension is given in Z.

$$Z = BX \quad (8)$$

$$\begin{pmatrix} Z_1 \\ \ldots \\ Z_m \end{pmatrix} = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ldots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix} \quad (9)$$

Eqn (8) and (9) represents the process compression using Bernoulli matrix. Following the process of compression the data are encoded using RLNC based coding technique to obtain new encoded data [23]. The encoding as well as decoding process comprised in RLNC technique is explained below.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Encoding process

- Initially, a matrix with the size of $1 \times N$ is obtained through converting the input data.
- Then, using the created dynamic permutation table the permutation of the generated matrix is performed. The dynamic permutation table is denoted as π_P.
- Following that the conversion of permuted data to its related sub matrices is attained using $\alpha = {}^{N}/_{h^2}$.The created sub matrix along with permutation is given as $SD = SD_1, SD_2 \ldots SD_\alpha$. Number of rows and columns present in this permuted sub matrix is given as h column and h row.
- Then, the selection of coefficient matrix from selection table is performed randomly. The selection table is represented as SG within the range of $(1 \times \alpha \; and \; NG \leq \alpha)$. Random number between 1 and NG is present within the selection table.
- By means of performing dot product between coefficients matrix along with permuted sub matrix the encoded sub-matrix is obtained. The mathematical expression for the generated encoded sub matrix is given in eqn (10) and (11).

$$C_{ij} = G_{ij} \odot PD_{ij} \tag{10}$$

$$C_{ij} = \begin{pmatrix} G_{11} & \cdots & G_{1h} \\ \vdots & \ldots & \vdots \\ G_{t1} & \cdots & G_{th} \end{pmatrix} \odot \begin{pmatrix} PD_{11} & \cdots & PD_{1h} \\ \vdots & \ldots & \vdots \\ PD_{h1} & \cdots & PD_{hh} \end{pmatrix} \tag{11}$$

- The size of created coefficient matrix is $t \times h$ and it should be invertible as well as possess coefficient within Galois field (2^8). The final output obtained after this process is new encoded data. The encoded data is further sent for storing in cloud.

Decoding process

- To retrieve the original data alike encoding process is performed by the user but in the reversal order. In this decoding process inverse coefficient matrix as well as inverse permutation matrix is generated.
- The extraction of encoded matrix from the sub-matrix is achieved. The size of the sub matrix considered is $h \times h$ and the encoded matrix from which the sub matrix is extracted is represented as C_{ij}. Finally, the extracted sub-matrix is denoted as Ch_{ij}.
- Following that the inverse of coefficient matrix is crossed with the obtained sub matrix. G_{ij}^{-1} is the expression used for representing the inverse coefficient matrix.

$$PD_{ij} = G_{ij}^{-1}.\odot Ch_{ij} \tag{12}$$

- Finally, to obtain original data the process of inverse permutation operation π_p^{-1} is performed.

Cloud storage

Massive data gathered from multiple user is encoded and then stored in cloud storage. Cloud is found to be an effective storage system and it renders numerous advantages for both corporate as well as private users. Normally, the cloud is a system in which data are stored and can be accessed through online by the user from anywhere. Cloud provide service to multiple users in terms of both compute and storage. So, in this present work the non-attack data is encoded and then stored in cloud. The users can access the data from cloud at any time and perform the operation decoding to obtain the original data. Although cloud is utilized by large amount of users security is still a major concern in cloud. Thus, the encoding operation is performed before storing in cloud.

3.5 DOS Attack Class

Controversially if the data is predicted as DOS attack class then it is further categorized into different types of DOS attack such as ping flood attack, TCP flood attack and so on. After categorizing the type of attack an alert message is sent to the user regarding the attack.

Based on this proposed deep learning based detection model, the presence of DOS attack within the network flow can be detected effectively. GRU functions better and achieves accurate detection when compared to other deep learning approach. After the detection of attack, the non-attack data is efficiently stored in cloud storage using MRLNC

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

encoding technique. On the other hand, the attack data alters the user regarding the prevailing attack. Therefore, attack free network can be developed using this proposed detection model. The performance of the proposed deep learning based prediction model is evaluated and the results obtained is discussed in the next portion.

4. RESULT AND DISCUSSION

Proposed deep learning based DOS detection model using GRU is implemented on MATLAB 2020b with Windows x64 bit platform, Intel Core i5 processor and 8 GB RAM. Dataset considered for analysing the proposed detection model is CAIDA "DDoS Attack 2007". The acquired dataset contains file in *pcap* format and further this *pcap* file is extracted to obtain *csv* file format. Around 2, 25,746 rows and 79 attributes are contained in the dataset. Some of the attributes included in the dataset are source IP, IP, source port, destination port, protocol type etc. dataset containing these rows and columns are processed further to detect DOS attack within the network.

As the acquired dataset consist of raw data, it is pre-processed using different pre-processing technique to reach meaningful data. The pre-processing technique used in this work is min-max normalization which normalize the entire data to a certain range for achieved ease detection using the classifier. Then, the pre-processed data is then sent for feature selection process in which the redundant features necessary for detection is selected using filter based feature selection technique namely fisher score. Feature selection process is carried out based on the threshold value. The selected features is sent as an input into GRU for classifying DOS attack and non-attack data.

The entire dataset containing 2, 25,746 samples as such is not given for detection around 80% of the sample is given for training process and remaining 20% of sample is given for testing process. Number of samples considered for training and testing is 180596 and 45149 samples. In GRU, at first the training process is performed using the training set and based on the knowledge acquired from training process, the next process of testing is carried out. Finally using this classifier, the DOS attack and non-attack data is detected. The user is sent a warning message if DOS attack is detected using GRU or else the data is stored in cloud. Here, the performance of GRU classifier is evaluated. Simulation parameter for GRU classifier is given in table 1.

Table 1: Simulation Parameter for GRU classifier

Parameters	Value
Input Size	auto
Number of Hidden Units	100
Output Mode	sequence
State Activation Function	tanh
Gate Activation Function	sigmoid
Reset Gate Mode	after-multiplication

Before performing the process of training and testing using the GRU classifier the parameter which are listed above is set. The performance of the classifier can be determine based on AUC plot. In addition to it the performance of the proposed GRU technique is compared with some of the existing deep learning techniques such as Long Short Term Memory (LSTM), Recurrent Neural Network (RNN), Deep Belief Network (DBN) and Deep Neural Network (DNN). AUC plot obtained for proposed and existing techniques is given in figure 3.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

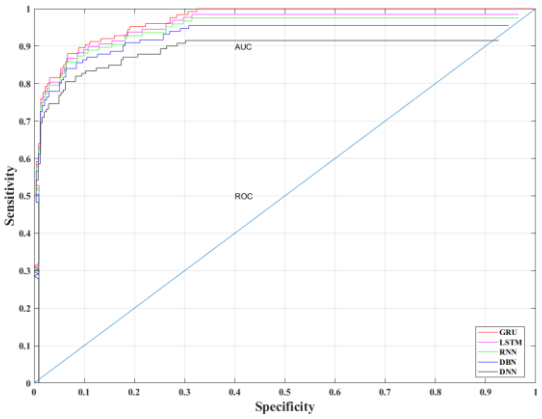

Figure 3: AUC Plot for Proposed and Existing Techniques

Area Under the Curve (AUC) - Receiver Operating Characteristics (ROC) curves are generally a statistic used for finding the performance and issue in the designed classifier at various levels of threshold. ROC represents the probability curve and AUC denotes the degree of separate. the performance of the classifier is determined to be good when the value for AUC is nearer to 1 and on the other hand the classifier performance is found to be low if the value for AUC is nearer to zero. To obtain the AUC plot, the graph is drawn between specificity and sensitivity. Calculation of true positive ratio with respect to false positive ratio at different level of threshold gives ROC curve. From the graph value of AUC for proposed GRU is 0.97 whereas for other existing techniques such as LSTM, RNN, DBN and DNN is 0.95, 0.94, 0.92 and 0.91. Analysis of AUC plot proves that the proposed classifier function better when contrast to existing. Some of the statistical parameters such as accuracy, kappa, recall, error, precision and so on are also used for evaluating the performance of the proposed model. To calculate these parameters the confusion matrix must be obtained. Table 2 illustrates the confusion matrix obtained for the proposed model.

Table 2: Confusion Matrix for Proposed Model

Techniques	**Actual class**	**Predicted class**	
		True	False
GRU	Positive	92300	6228
	Negative	7336	75623

From the above mentioned confusion matrix it is inferred that using GRU classifier around 92300 samples are correctly predicted as class 0 and 6228 samples are incorrectly predicted as class 0. Following that around 75623 samples are correctly predicted as class 1 and 7336 samples are incorrectly predicted as class 1. However only little samples from both the classes are incorrectly predicted. This shows that improved DOS attack detection is determine to be achieved using the proposed deep learning model. Using this confusion matrix the evaluated statistical parameter are represented in graphical format and given in below figures.

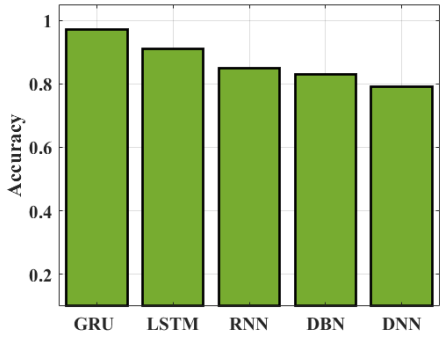

Figure 4: Accuracy Comparison between Proposed and Existing DOS Detection Model

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Accuracy parameter is calculated for the proposed GRU based DOS detection model based on confusion matrix and then compared with some of the existing deep learning approaches. This accuracy comparison plot is given in figure 4. This figure is sketched between various deep learning techniques X label and value obtained for accuracy in percentage on Y label. For proposed GRU model obtained accuracy value is 93%. Whereas for other existing models such as LSTM, RNN, DBN and DNN the accuracy value is 91%, 85%, 83% and 79%. This accuracy plot revels that GRU model function better in DOS attack detection when compared to another existing DOS detection model.

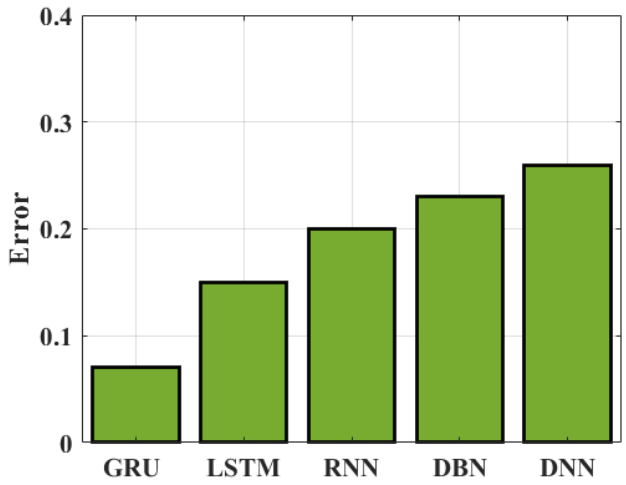

Figure 5: Error Comparison between Proposed and Existing DOS Detection Model

Calculation and comparison of error metrics between proposed and existing DOS attack detection model is given in figure 5. The error metric plot is drawn using various techniques and error value on both the axes respectively. Error value reached for proposed GRU based DOS detection model is 7%. Following that error value reached for remaining existing model like LSTM, RNN, DBN and DNN is 9%, 15%, and 17% and 21%. This error comparison illustrates that only lesser error probability is attained by the proposed GRU based DOS detection model.

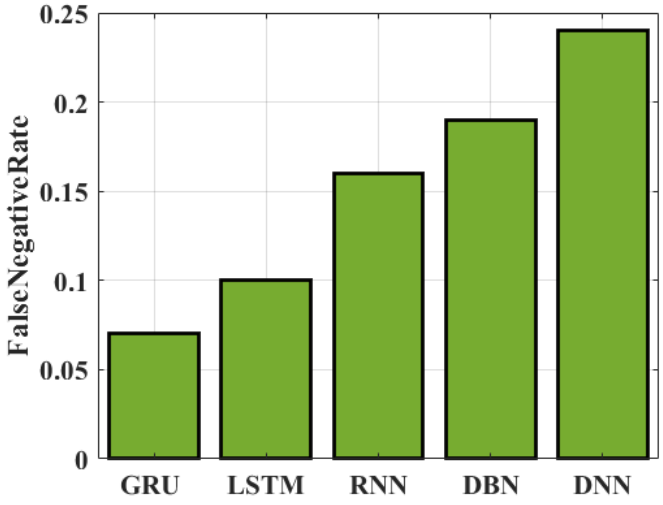

Figure 6: FNR Comparison between Proposed and Existing DOS Detection Model

Proposed GRU based detection model is compared with some of the existing detection model using False Negative Rate (FNR) parameter. This FNR parameter comparison is given in Figure 6. In this figure various deep learning techniques used for DOS detection is plotted in X-axis and FNR in terms of percentage is plotted in Y-axis. 7% is the FNR value achieved for the proposed GRU based detection model. Subsequently, 10%, 16%, 19% and 24% is the FNR value achieved for the existing techniques such as LSTM, RNN, DBN and DNN.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

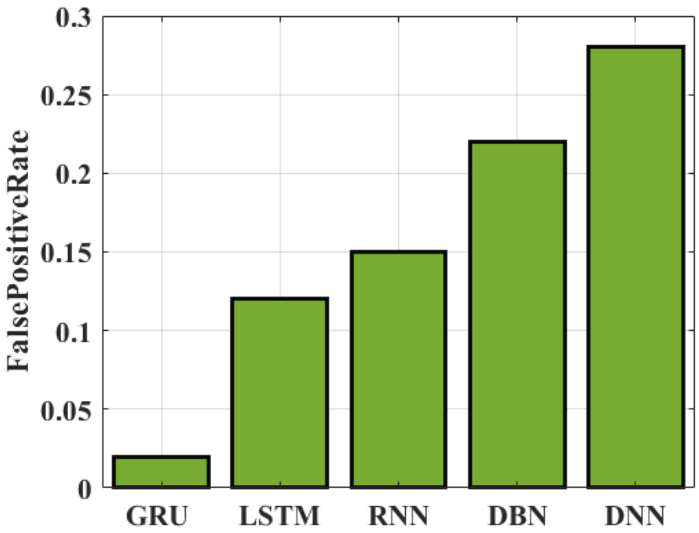

Figure 7: FPR Comparison between Proposed and Existing DOS Detection Model

Figure 7 illustrates the comparison of False Positive Rate FPR metric among proposed and existing DOS detection model. FPR graph is drawn between various DOS detection model and FPR value on X and Y axis respectively. Value of FPR attained for the proposed DOS detection model is 2%. Similarly, value of FPR attained for other existing DOS detection model such as LSTM, RNN, DBN and DNN is 12%, 15%, 22% and 28%. Lesser value for FPR proves that data samples are correctly predicted using the proposed DOS detection model.

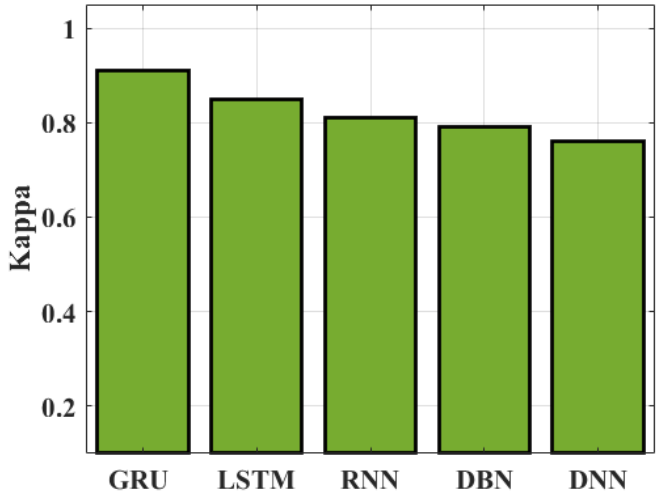

Figure 8: Kappa Comparison between Proposed and Existing DOS Detection Model

Comparison of kappa metrics between proposed and existing DOS detection model is given in figure 8. This comparison graph is drawn between various techniques on X axis and kappa metrics on Y axis. Kappa value determine for the proposed DOS detection model is 91%. Whereas for other existing DOS detection model like LSTM, RNN, DBN and DNN kappa value is determine to be 85%, 81%, 79% and 76%. This comparison shows that proposed GRU based detection model functions effectively in detecting DOS attack.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

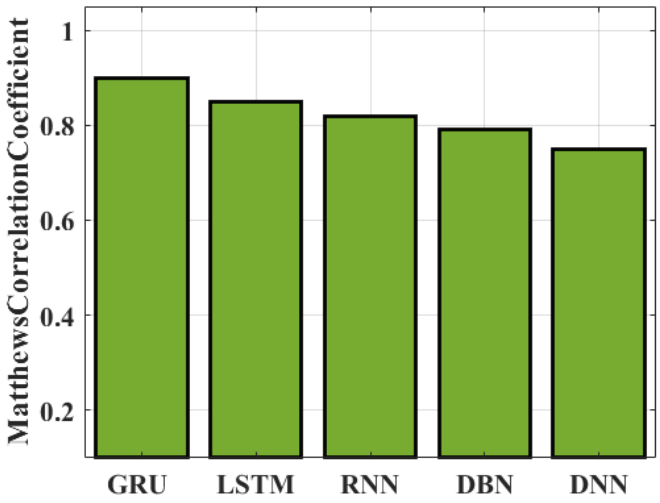

Figure 9: MCC Comparison between Proposed and Existing DOS Detection Model

MCC metric is calculated for proposed GRU based detection model and then compared with some of the existing deep learning models. The graph for this comparison study is given in figure 9 and it is plotted between different deep learning techniques and MCC metric on both the axes respectively. The calculated MCC value for the proposed DOS detection model is 90%. Then, for the remaining existing model such as LSTM, RNN, DBN and DNN the calculated MCC metric is 85%, 82%, 79% and 75%.

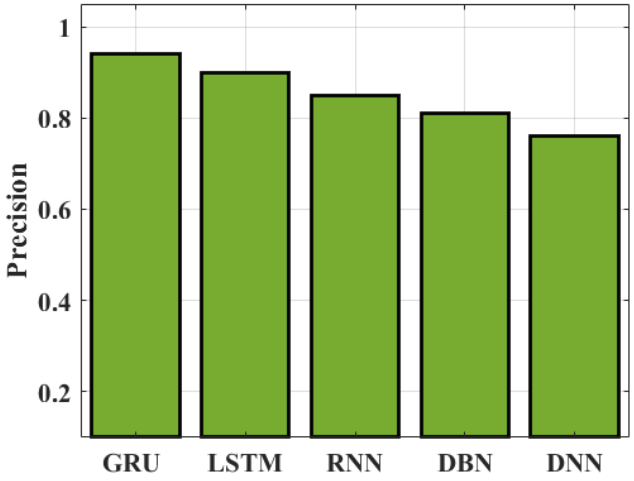

Figure 10: Precision Comparison between Proposed and Existing DOS Detection Model

Figure 10 displays the comparison study carried out using the proposed DOS detection model and existing detection model for precision metric. The graph is plotted between various deep learning technique and precision in percentage on both axes respectively. The precision value obtained for proposed GRU based DOS detection model is 94% while for other existing DOS detection models such as LSTM, RNN, DBN and DNN the value of precision is 90%, 85%, 81% and 76%.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

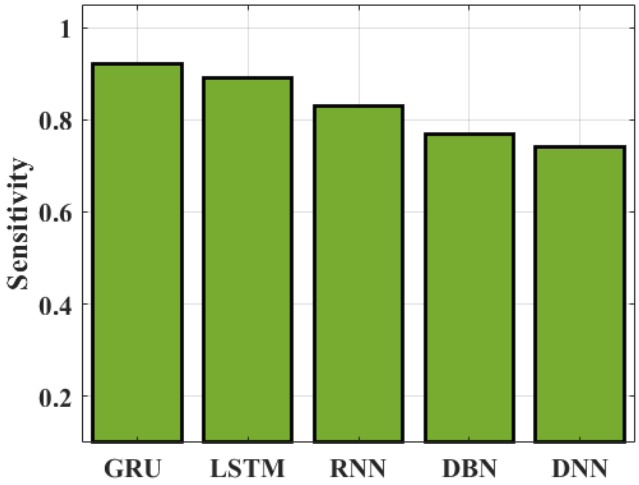

Figure 11: Sensitivity Comparison between Proposed and Existing DOS Detection Model

Sensitivity of proposed and existing DOS detection model is compared and sketched in figure 11. Because it properly gauges the positive data set, sensitivity is essential for detecting network activity. The suggested methods are more sensitive and are used to find little changes in a server's network. In comparison to the proposed model, the existing model are found to be less sensitive. The sensitivity of the proposed DOS detection model is 92%%, and the sensitivity value of existing DOS detection model such as LSTM, RNN, DBN and DNN is 89%, 83%, 77% and 74% respectively.

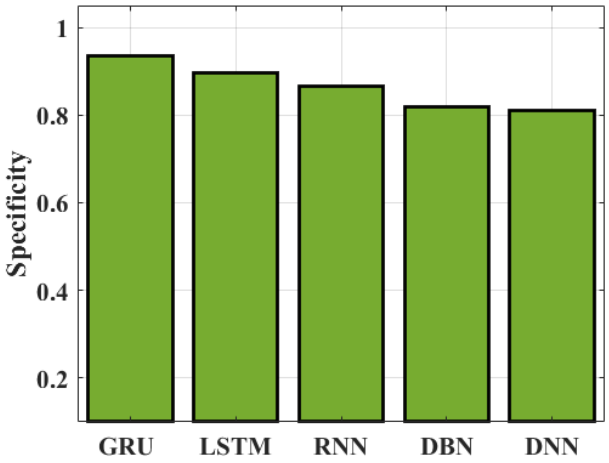

Figure 12: Sensitivity Comparison between Proposed and Existing DOS Detection Model

Comparison study done using sensitivity metric between proposed DOS detection model and existing model is provided in figure 12. Similarly, in this also the graph is plotted between various detection model and specificity value in percentage on X label and Y label respectively. The specificity value reached for the proposed DOS detection model is 93% whereas for existing prediction model such as LSTM, RNN, DBN and DNN the specificity value is determined to be 89%, 83%, 77% and 74%.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

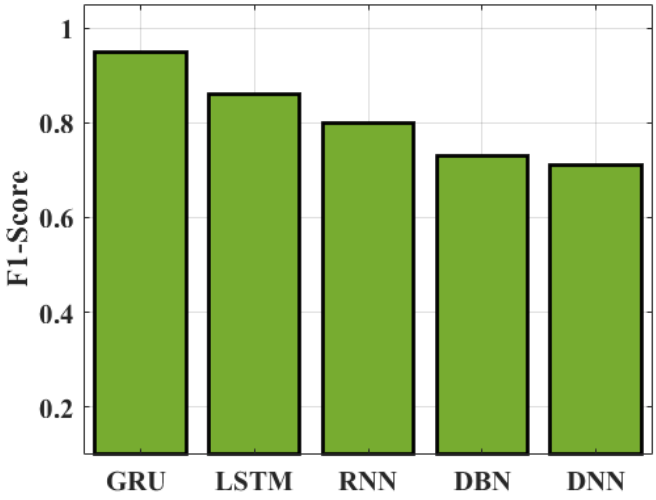

Figure 13: F1 score Comparison between Proposed and Existing DOS Detection Model

The comparison of F1 score between proposed DOS detection model and existing detection model is given in figure 13. It is plotted between different deep learning techniques and F1 Score metric on both the axes respectively. The F1 score metric obtained for the proposed GRU based DOS detection model is 95% and for existing model such as LSTM, RNN, DBN and DNN the value of F1 score is 86%, 80%, 73% and 71%.

5. CONCLUSION

Malicious behaviour is one of the important reasons for arising various security threats in the network. Detection and isolation of these abnormal activity within the network is essential to improve the network performance. Traditionally, Intrusion Detection System (IDS) and firewall was used to detect DOS attack in the network. However due to presence of complex attacking methods detection using IDS system is ineffective. So, for achieving effective detection of DOS attack within the network AI system is introduced. In AI system, machine learning is the most commonly used technique for DOS attack detection. As the data for detection is collected from heavy network traffic low detection rate is attained using ML. so, for attaining improved detection rate deep learning enabled DOS attack model is developed. The raw data is pre-process initially using min-max normalization. Then, optimal features for classification is selected using fisher score method. Fisher score method functions effectively on using high dimensionality data. The selected features is sent as input into GRU for detection. The non-attack data is further processed using MRLNC and stored in cloud. On the other hand, the attack data is then categorized into different types of attacks to alter the users. Simulation analysis done on the proposed model showed effective functioning in DOS attack detection when compared to other existing attack detection model.

REFERENCES

1. Baig, Z. A., Sanguanpong, S., Firdous, S. N., Nguyen, T. G., & So-In, C. (2020). Averaged dependence estimators for DoS attack detection in IoT networks. Future Generation Computer Systems, 102, 198-209.
2. Dwivedi, S., Vardhan, M., & Tripathi, S. (2022). Defense against distributed DoS attack detection by using intelligent evolutionary algorithm. International Journal of Computers and Applications, 44(3), 219-229.
3. Tan, Z., Jamdagni, A., He, X., Nanda, P., & Liu, R. P. (2013). A system for denial-of-service attack detection based on multivariate correlation analysis. IEEE transactions on parallel and distributed systems, 25(2), 447-456.
4. Qu, X., Yang, L., Guo, K., Ma, L., Feng, T., Ren, S., & Sun, M. (2019). Statistics-enhanced direct batch growth self-organizing mapping for efficient DoS attack detection. IEEE Access, 7, 78434-78441.
5. Tang, D., Dai, R., Tang, L., & Li, X. (2020). Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis. Human-centric Computing and Information Sciences, 10(1), 1-20.
6. Kshirsagar, D., & Kumar, S. (2021). An efficient feature reduction method for the detection of DoS attack. ICT Express, 7(3), 371-375.

7. Latah, M., & Toker, L. (2020). Minimizing false positive rate for DoS attack detection: A hybrid SDN-based approach. ICT Express, 6(2), 125-127.
8. Anand, C., & Gnanamurthy, R. K. (2016). Localized DoS attack detection architecture for reliable data transmission over wireless sensor network. Wireless Personal Communications, 90(2), 847-859.
9. Zhang, Y. Y., Li, X. Z., & Liu, Y. A. (2012). The detection and defence of DoS attack for wireless sensor network. The journal of china universities of posts and telecommunications, 19, 52-56.
10. AP, H. (2019). Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. EURASIP Journal on Wireless Communications and Networking, 2019(1), 1-15.
11. Anand, C., & Vasuki, N. (2021). Trust Based DoS Attack Detection in Wireless Sensor Networks for Reliable Data Transmission. Wireless Personal Communications, 121(4), 2911-2926.
12. Adi, E., Baig, Z., & Hingston, P. (2017). Stealthy Denial of Service (DoS) attack modelling and detection for HTTP/2 services. Journal of Network and Computer Applications, 91, 1-13.
13. Kachavimath, A. V., & Narayan, D. G. (2021). A deep learning-based framework for distributed denial-of-service attacks detection in cloud environment. In Advances in computing and network communications (pp. 605-618). Springer, Singapore.
14. Ferrag, M. A., Shu, L., Djallel, H., & Choo, K. K. R. (2021). Deep learning-based intrusion detection for distributed denial of service attack in Agriculture 4.0. Electronics, 10(11), 1257.
15. Xu, C., Shen, J., & Du, X. (2021). Low-rate DoS attack detection method based on hybrid deep neural networks. Journal of Information Security and Applications, 60, 102879.
16. Ramesh, S., Yaashuwanth, C., Prathibanandhi, K., Basha, A. R., & Jayasankar, T. (2021). An optimized deep neural network based DoS attack detection in wireless video sensor network. Journal of Ambient Intelligence and Humanized Computing, 1-14.
17. Premkumar, M., & Sundararajan, T. V. P. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. Microprocessors and Microsystems, 79, 103278.
18. NG, B. A., & Selvakumar, S. (2019). Deep radial intelligence with cumulative incarnation approach for detecting denial of service attacks. Neurocomputing, 340, 294-308.
19. Gormez, Y., Aydin, Z., Karademir, R., & Gungor, V. C. (2020). A deep learning approach with Bayesian optimization and ensemble classifiers for detecting denial of service attacks. International Journal of Communication Systems, 33(11), e4401.
20. Kasim, Ö. (2020). An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks. Computer Networks, 180, 107390.
21. Singh, B., Sankhwar, J. S., & Vyas, O. P. (2014, December). Optimization of feature selection method for high dimensional data using fisher score and minimum spanning tree. In 2014 annual IEEE India conference (INDICON) (pp. 1-6). IEEE.
22. Ke, K., Hongbin, S., Chengkang, Z., & Brown, C. (2019). Short-term electrical load forecasting method based on stacked auto-encoding and GRU neural network. Evolutionary Intelligence, 12(3), 385-394.
23. Tassi, A., Chatzigeorgiou, I., & Lucani, D. E. (2015). Analysis and optimization of sparse random linear network coding for reliable multicast services. IEEE Transactions on Communications, 64(1), 285-299.
24. Sahoo, K. S., Tripathy, B. K., Naik, K., Ramasubbareddy, S., Balusamy, B., Khari, M., & Burgos, D. (2020). An evolutionary SVM model for DDOS attack detection in software defined networks. IEEE access, 8, 132502-132513.
25. Agrawal, A., Singh, R., Khari, M., Vimal, S., & Lim, S. (2022). Autoencoder for Design of Mitigation Model for DDOS Attacks via M-DBNN. Wireless Communications and Mobile Computing, 2022(1), 9855022.
26. Agarwal, A., Khari, M., & Singh, R. (2022). Detection of DDOS attack using deep learning model in cloud storage application. Wireless Personal Communications, 1-21.
27. Agarwal, A., Singh, R., & Khari, M. (2022, April). Detection of DDOS attack using IDS mechanism: a review. In 2022 1st International conference on informatics (ICI) (pp. 36-46). IEEE.